COUNCIL OF
THE EUROPEAN UNION

Brussels, 17 November 2010

15457/10

COPEN 237
JURINFO 50
EJUSTICE 105

NOTE

from:	General Secretariat of the Council
to:	Delegations
Subject:	ECRIS Technical Specifications - Security Analysis

Delegations will find in the Annex the revised text of the ECRIS Technical Specifications - Security Analysis, as agreed on at the Working Party on Cooperation in Criminal matters which met on 20 October 2010.

ANNEX

European Commission – DG Justice

iLICONN Consortium (Bilbomatica – Intrasoft – Unisys)

ECRIS Technical Specifications

Security Analysis

Document Information

AUTHOR	iLICONN – Intrasoft International S.A.
OWNER	European Commission – DG Justice
ISSUE DATE	22/10/2010
VERSION	1.0
APPROVAL STATUS	Adopted

Authors

NAME	ACRONYM	ORGANISATION	ROLE
Marc LOMBAERTS	MLO	iLICONN – Unisys Belgium	Main Author
Nicholas YIALELIS	NYI	iLICONN – Intrasoft International S.A.	Manager Reviewer
Ludovic COLACINO DIAS	LCO	iLICONN – Intrasoft International S.A.	Contributor Reviewer
Panos ATHANASIOU	PAT	iLICONN – Intrasoft International S.A.	Contributor
Michel HOFFMANN	MHO	iLICONN – Unisys Belgium	Reviewer

Document History

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	06/09/2010	MLO	First draft
0.2	09/09/2010	PAT LCO NYI	Contributions and revision
0.3	10/09/2010	MLO	Second draft
0.4	10/09/2010	LCO	Finalisation of the proposals document
0.5	21/09/2010	MLO	Third draft
0.6	23/09/2010	PAT MLO	Modification of sections 5.4.7 and 5.4.8. Review document following the feedback and comments from the technical experts of the MS.
0.7	26/09/2010	NYI	Revision
0.8	27/09/2010	LCO	Finalisation before delivery
0.9	14/10/2010	NYI LCO	Implementation as per author’s position in “Inspection Sheet” v1.2
1.0	22/10/2010	LCO	Text of version 0.9, adopted in Council by COPEN Working Party on 20-Oct-2010

TABLE OF CONTENTS

DOCUMENT

1.1 Purpose

This document is a formal product of the *ECRIS Technical Specifications* project for the European Commission – DG Justice and produced by the iLICONN Consortium.

The main purpose of this document is to analyse objectively the risks of potential security breaches that might occur during the exchange of criminal records information using ECRIS. It aims at identifying avoidance, transfer and mitigation actions where possible and proposes technical alternatives that are to be implemented at the level of the *ECRIS Technical Specifications*.

This document assumes that the readers have a good and detailed knowledge and understanding of the following elements:

- ECRIS legal basis
- The "ECRIS Technical Specifications – Inception Report" document

1.2 Scope

The scope of the study is limited to the risks that could occur during the exchange of information extracted from criminal records between ECRIS applications of Member States, as described in the "Inception Report" document.

The exchange of information relies on sTESTA, which is a secure network providing European public administrations with a controlled communications environment to exchange administrative information with guaranteed performance levels.

The main output is a description of the risks that will need to be mitigated by specific security measures and a description of technical and operational measures for minimising risk exposure.

1.3 References

The following documents have been used as input to the security analysis presented in this document:

[1] ECRIS Legal Basis – Council Framework Decision 2009/315/JHA
Council of the European Union (2009), Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93/23 of 07.04.2009).

[2] ECRIS Legal Basis – Council Decision 2009/316/JHA
Council of the European Union (2009), Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93/33 of 07.04.09).

[3] European Commission – DG Enterprise (2004): IDA Architecture Guidelines for Trans-European Telematics Networks for Administrations, version 7.1 of 13 February 2004 (and annexes).

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[5] Expression des Besoins et Identification des Objectifs de Sécurité : Base de connaissances, 25 janvier 2010, (http://www.ssi.gouv.fr/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf).

[6] ECRIS Technical Specifications – Inception Report v1.02 of 22 October 2010

[7] ECRIS Technical Specifications – Technical Architecture v1.0 of 22 October 2010

[8] Comments on the "ECRIS Security Proposals" received from the following Member States: BE, DE, EE, EL, ES, FR, LU, RO, SE, SK, UK

[9] ECRIS Technical Specifications - Expert Sub Group Meeting Minutes and Conclusions of 22 September 2010

[10] ECRIS Technical Specifications – Glossary v1.0 of 05 October 2010

[11] Michael Burrows , Martin Abadi , Roger Needham, A logic of authentication, ACM Transactions on Computer Systems (TOCS), v.8 n.1, p.18-36, Feb. 1990

[12] B. Lampson, M. Abadi, M. Burrows, and E. Wobber. Authentication in distributed systems: Theory and practice. ACM Trans. Computer Systems 10, 4 (Nov. 1992), pp 265-310.

[13] Cryptography Engineering, Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, John Wiley & Sons, March 15, 2010, ISBN: 9780470474242

[14] Web Services Security: SOAP Message Security 1.1, (WS-Security 2004), OASIS Standard Specification, 1 February 2006 (http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf)

[15] "Interoperability with Microsoft WCF/.NET - WS-Security Interoperability Guidelines
Oracle Technology Network Documentation
(http://download.oracle.com/docs/cd/E12840_01/wls/docs103/webserv_intro/interop.html#wp217472)

[16] "Guide to secure Web Services"
Anoop Sighal, Theodore Winograd, Karen Scarfone - (2007 - NIST)
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

[17] "Man-in-the-middle attack"
OWASP - 23/4/2009
http://www.owasp.org/index.php/Man-in-the-middle_attack

[18] DIN ISO/IEC 27002:2008-09 (E) Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005).

1.4 About this Document

1.4.1 *Elaboration of this Document*

This “Security Analysis” document has been drafted by the iLICONN project team based on the following input:

§ The documents listed in the references above

§ The answers provided by the following Member States’ central authorities to the concrete proposals described in the “ECRIS Security Proposals” document that has been sent out by iLICONN to all Member States’ contact points on the 13th of September 2010 (listed in alphabetical order):

Belgium (BE), the Czech Republic (CZ), France (FR), Germany (DE), Greece (GR), Luxembourg (LU), Romania (RO), Slovakia (SK), Spain (ES), Sweden (SE), the United Kingdom (UK)

- The discussions and conclusions that have been reached during the Expert Sub Group Meeting on 22nd of September 2010 with the technical experts of the following Member States:
  DE, EE, ES, LT, UK
- The comments issued by the Member States on the previous version of this document by the 06th of October 2010.

1.4.2 *Understanding this Document*

This document comes with a “Glossary” document that provides definitions for the specific terms that are used throughout the *ECRIS Technical Specifications* project.

By convention, all words marked in italic in this document can be looked up in the “Glossary” document. The bold font is used for emphasising a specific term or part of a sentence. The underlines mark the text that has been added or modified since the last version while the strike-through marks the text that has been removed or replaced.

In case of doubts about the exact meaning of a term, please consult first the “Glossary”.

Should you still have any doubts about the meaning of a specific sentence or paragraph, please do not hesitate to take direct contact with the following persons by telephone or via e-mail, at your best convenience:

Organisation: European Commission – DG Justice – Criminal Law
Name: Jaime LOPEZ-LOOSVELT
E-mail: JUST-CRIMINAL-RECORD@ec.europa.eu
Telephone: +32 (0)2.298.41.54

Organisation: iLICONN Consortium – Intrasoft International S.A.
Name: Ludovic COLACINO DIAS
E-mail: ECRIS-Specs-PM.iLICONN@intrasoft-intl.com
Mobile: +32 (0)498.30.25.55

1.4.3 *Providing Comments*

As described in the "Inception Report" document, all major deliverables produced by the iLICONN Consortium are undergoing a "Review Cycle" during which all EU Member States experts are invited to provide comments.

Since the iLICONN staff needs to collect, compare and analyse the feedback from 27 Member States on the same document – thus potentially a large number of comments – it uses a tool that allows easily extracting the comments from MS Word documents.

Therefore, for commenting this document, please apply the following guidelines:

- All comments are to be written in plain English. Comments provided in other languages cannot, unfortunately, be taken into account.
- The comments must be specific to and must relate to the text (sentence and/or paragraph) being revised.
- Please use simple wording and be as specific, concise and clear as possible in order to avoid ambiguities.
- When referring to specific terms, acronyms, abbreviations that are common in your daily jargon but that are not defined in the *Glossary* document, please define them first.
- Write your comments directly in this MS Word document, by proceeding as follows:
  - First select a word, a part of a sentence or a paragraph (this can be done for example by double-clicking on a word or by dragging your mouse over parts of the text while keeping the left mouse-button pressed).

    Attention:

    Please note that a **minimum of 4 characters** must be selected in order for our commenting tool to grab the comment. Furthermore, comments on diagrams and embedded pictures are also not taken into account. In such cases, please select the caption text underneath the diagram or image.

- Once a word, part of a sentence or paragraph has been selected, insert an MS Word comment in which you can type your remarks.

  An MS Word comment is typically displayed as a red balloon in the right margin of the document and usually starts with the abbreviation of your name and the timestamp at which the comment is being written. Depending on your version of MS Word, use the following steps for inserting a comment:

  MS Word 2007 and MS Word 2010:

  1. Select the text you would like to comment upon
  2. Open the **Review** ribbon, select **New Comment** in the **Comments** section
  3. In the balloon that appears in the right margin, type your comment
  4. Click anywhere in the document to continue editing the document

  MS Word 2003:

  1. Select the text you would like to comment upon
  2. From the **Insert** menu, select **Comment** (or click on the **New Comment** button on the **Reviewing** toolbar)
  3. In the balloon that appears in the right margin, type your comment
  4. Click anywhere in the document to continue editing the document

  The text will have coloured lines surrounding it, and a dotted coloured line will connect it to the comment. To delete a comment, simply right click on the balloon and select **Delete Comment**.

§ Please do not use the MS Word “track changes” tool and do not write your comments as plain text in the MS Word file.

§ In case that you want to provide general comments or remarks that are not specific to a part of the text of this document, please provide them into a separate document and/or e-mail.

In case that you need to translate this document to another language, and then translate back your comments to English, please make sure that your comments are provided in the form described above and that they have not been altered or moved to another section of the text during the translation process.

Approach

The scope of this risk assessment is to identify and assess the risks that may affect the security of criminal records information exchanged between Member States in the frame of the ECRIS project.

The risk assessment is performed in steps as follows:

- Define the assets that will be considered in the scope of the study.
- Identify the needs in term of security arising from the ECRIS legal basis.
- Identify the relevant threats in the context of exchanges of criminal records information. These threats are selected from the Knowledge Base of EBIOS 2010. EBIOS stands for “Expression des Besoins et Identification des Objectifs de Sécurité”. This method is published by the “Direction Centrale de la Sécurité des Systèmes d'Information” (DCSSI) of the French government.
- Evaluate the associated risk exposure for each threat by:
  - Estimating the impact on the assets;
  - Estimating the probability that a threat may occur;
  - Associating the estimated impacts and probabilities for determining the risk exposure and the corresponding priority.
- Provide a list of measures to mitigate the risk.
- Describe the mitigation measures in more detail.

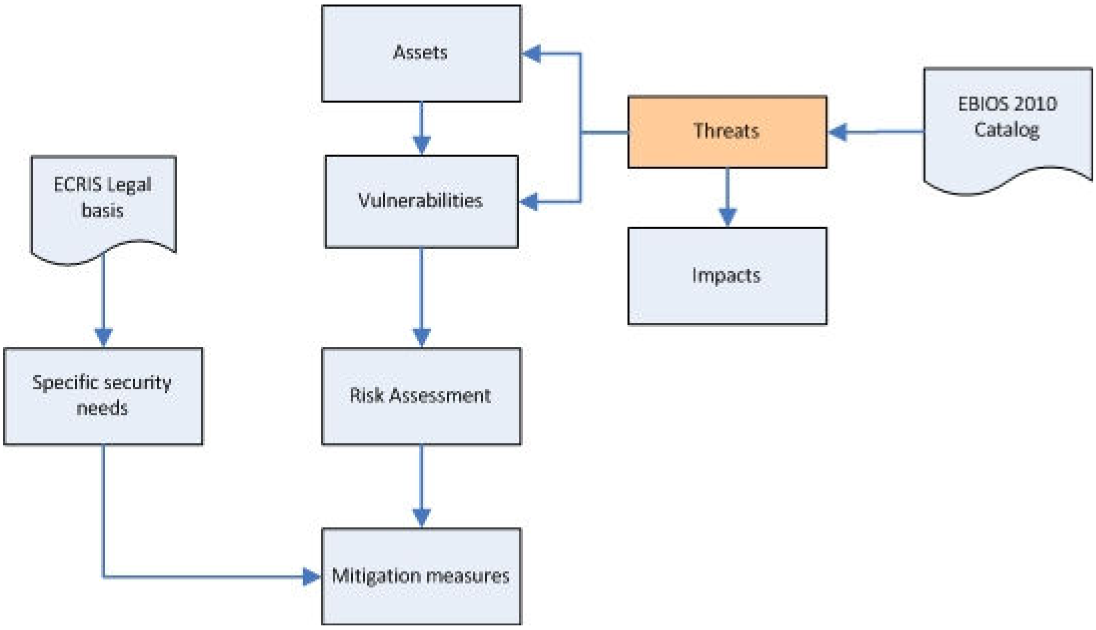

Figure 1 – Study approach

System Definition

1.5 Role and Architecture of the System

ECRIS is to be used for exchange information on convictions stored in the local criminal record registers (CRR) of the Member States. The communication is to be done on a peer-to-peer basis between the 27 Member States. The figure below gives an overview of the communication network on which ECRIS is based.

Each request initiated by the central authority (CA) of a Member State transits through the national networks of the requesting and the requested Member States and through the sTESTA network. sTESTA is a secure backbone network ensuring confidentiality and integrity by encrypting the data on network level (IPSec) as well as availability of the network by offering a high availability architecture (redundancy of the lines and access points).

The national networks do not usually encrypt the data, which means that the information may be transmitted in clear text in certain parts of its route if no additional measures are taken.

It is noted that the IT processing systems and assets (such as servers, software, etc.) and the end users of the ECRIS applications are under the responsibility of the Member States and thus they are not included in the scope of the present analysis. Furthermore no central storage or processing of any data is foreseen.

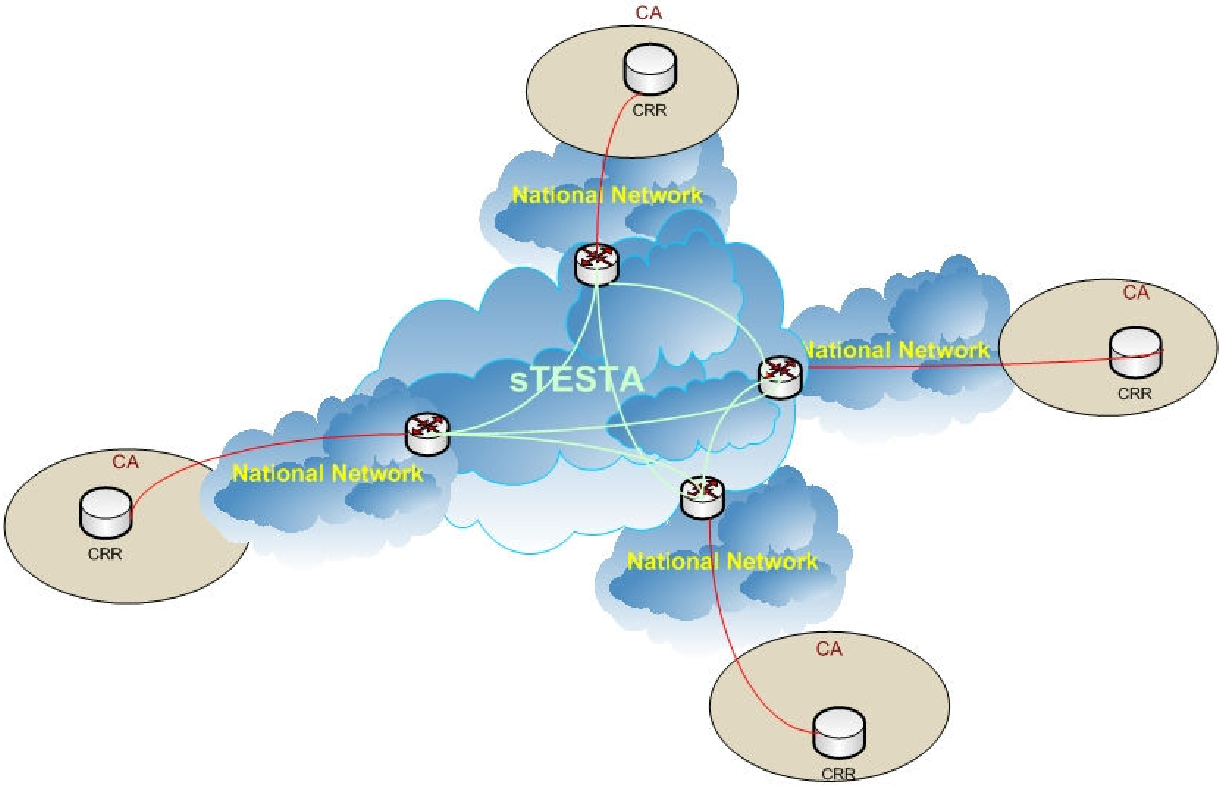

Figure 2 – ECRIS communication network

1.6 Assets

Two types of assets have to be considered in the context of this security study as follows:

§ The first type of asset concerns the electronic services provided by each Member States' central authority for effectively performing the exchange of information extracted from the criminal records as per the ECRIS legal basis, namely (1) the communication network, including the sTESTA backbone network and the segments of the national networks connecting the central authority site to the national sTESTA access point and (2) the piece of software that sends and receives the ECRIS data.

§ The second type of asset concerns the information itself being exchanged between the Member States. This information includes 3 types of data elements as expressed in the ECRIS legal basis:

1. Obligatory information:
   - i. Information of the convicted person: full name, date of birth, place of birth (town and State), gender, nationalities and, if applicable, previous name(s).
   - ii. Information on the nature of the conviction: date of conviction, name of the court, date on which the decision became final.
   - iii. Information on the offence giving rise to the conviction: date of offence, name or legal classification of the offence, references to the applicable legal provisions.
   - iv. Information on the contents of the conviction: the sentence, any supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence.
2. Optional information:
   - i. Convicted person's parent's names;
   - ii. Reference number of the conviction;
   - iii. Place of the offence;
   - iv. Disqualifications arising from the conviction.
3. Additional information:
   - i. Convicted person's identity number, or the type and number of the person's identification document;
   - ii. Fingerprints of the convicted person;
   - iii. Pseudonym and/or aliases.

The security study aims at defining measures for protecting the assets defined above; it does not, however, distinguish among the three types of information and thus no further reference to these types of information is given. It is assumed that any information exchanged between the Members States requires the same degree of security.

Security Requirements

1.7 Security Qualities Requirements

The purpose of this section is to extract from the ECRIS legal basis the security needs.

The table below lists the provisions of the ECRIS legal basis that are applicable in the scope of the present security analysis. In particular, it elaborates the security qualities that are required in ECRIS:

REFERENCE	ID	LEGAL BASIS TEXT	ANALYSIS	REQUIREMENT
Ref [1] Article 7, 1	LEG_01	**Reply to a request for information on convictions** "When information extracted from the criminal record is requested under Article 6 from the central authority of the Member State of the person's nationality for the purposes of criminal proceedings, that central authority **shall transmit to the central authority of the requesting Member State information on**: (a) convictions handed down in the Member State of the person's nationality and entered in the criminal record; […]	The use of "shall transmit" expresses a certain obligation of the requested Member State to answer to the requesting Member States.	***Non-Repudiation of Receipt***: the system shall provide sufficient means to allow the requesting Member State to prove that a given request was indeed well received at a certain time by the requested Member State.
Ref [1] Article 8, 1	LEG_02	**Deadlines for reply** "Replies to the requests referred to in Article 6(1) shall be transmitted by the central authority of the requested Member State to the central authority of the requesting Member State **immediately and in any event within a period not exceeding ten working days from the date the request was received,** […]	This article implies that there is a need in terms of **availability** of the system which corresponds to a period of ten working days.	**Service availability:** The service provided by any Member States to other Member States shall not be unavailable for more 10 working days (as per the calendar of at the requested Member State). It is clarified that the notion of a service in this context refers to the service provided by the systems, people and procedures as a whole. The availability requirement for the systems alone should define a maximum period of unavailability of less than 10 days but the exact number of days may differ from Member State to Member State and it is beyond the scope of this document to define.

Ref [1] Articles 9, 1 to 3	LEG_03	**Conditions for the use of personal data** "1.Personal data provided under Article 7(1) and (4) for the purposes of criminal proceedings may be **used by the requesting Member State only for the purposes of the criminal proceedings for which it was requested**, as specified in the form set out in the Annex. 2. Personal data provided under Article 7(2) and (4) for any purposes other than that of criminal proceedings may be used by the requesting Member State in accordance with its national law **only for the purposes for which it was requested** and within the limits specified by the requested Member State in the form set out in the Annex. 3. Notwithstanding paragraphs 1 and 2, personal data provided under Article 7(1), (2) and (4) may be used by the requesting Member State for **preventing an immediate and serious threat to public security."**	This has an indirect impact on the **"need-to-know"** concept as only requests for valid purposes shall be sent to a Member State. Requests for other purposes than the ones foreseen in the ECRIS legal basis and by the applicable regulations (e.g. criminal collusion, personal curiosity, public diffusion…) must be avoided. The mechanisms or procedures for making a decision as to whether a request is valid or not is beyond the scope of the present analysis. However, the system shall support **non-repudiation of origin** as a measure to prevent transmission of invalid requests.	***Non-Repudiation of Origin*****:** the system shall provide sufficient means to allow the requested Member State to prove that a given request was sent at a certain time by the requesting Member State.

Ref [2] Articles 3, 1b and 3	LEG_04	"ECRIS is a decentralised information technology system based on the criminal records databases in each Member State. It is composed of the following elements: […] (b) a common communication infrastructure that provides an **encrypted network**." "…The best available techniques identified together by Member States with the support of the Commission shall be employed **to ensure the confidentiality and integrity of criminal records information transmitted** to other Member States."	The legal basis calls for the usage of an encrypted network to exchange information on criminal records. For the purposes of this document, this is interpreted as a requirement that the data transmitted between national systems shall be encrypted. It is also understood that the legal basis calls for a high degree of protection against loss of the confidentiality and integrity of the transmitted data and requires the usage of the best available techniques.	**a. Data Confidentiality:** the system shall offer a high degree of protection against unauthorised disclosure during transmission between the central authorities of the Member States. **b. Data Integrity:** the system shall offer a high degree of protection against unauthorised modification during transmission between the central authorities of the Member States. It is clarified that protection in this context means that the receiver can verify that the data received are exactly the data sent by the claimed sender and that any alteration of the data will be understood by the receiver. **c. Use of Encryption:** Criminal Records information shall be exchanged between the central authorities in encrypted form.

Table 1 – Identification of security requirements

The table above identifies five **security qualities** that are implied as requirements by the ECRIS legal basis:

1. Data Confidentiality;
2. Data Integrity;
3. Service Availability;
4. *Non-Repudiation of Origin*;
5. *Non-Repudiation of Receipt*.

In addition, the table above identifies a technical requirement implied by the ECRIS legal basis: "the criminal records information should be exchanged in encrypted form between the central authorities".

It is noted that, in order to achieve data confidentiality and integrity, it is necessary to provide the means for proper authentication of the communicating parties. In this analysis authentication is not listed as a requirement but as a tool to achieve confidentiality and integrity (please refer to section §5.3 below).

1.8 Impact of Loss of Security Qualities

This section briefly describes the impacts that the loss of each of the security qualities identified above would have on ECRIS as a system.

1.8.1 *Loss of Confidentiality*

The loss of confidentiality would mean that the information extracted from the criminal records registers of the Member States would be disclosed to unauthorised persons. This would imply the following consequences:

- Violation of the ECRIS legal basis (LEG_04);
- Violation of the regulations on the protection of personal data;
- Potential loss of trust between Member States' central authorities.

1.8.2 *Loss of Integrity*

The loss of integrity would mean that the information on personal data and/or of convictions transmitted between Member States has suffered from loss of consistency or from unauthorised and unexpected modifications between the moment it was sent and the moment when it was received. This would imply the following consequences:

- Violation of the ECRIS legal basis (LEG_04);
- Loss of effectiveness of the ECRIS system;
- Potential corruption of the criminal records registers of the Member States;
- Wrong information on convictions, leading to inappropriate penal decisions;
- Deliberate disinformation for malicious purposes.

1.8.3 *Loss of Availability*

The loss of availability would mean that the service provided by at least one Member State is unavailable for more than 10 working days. This would imply the following consequences:

- Violation of the ECRIS legal basis (LEG_02);
- Requests and responses to requests not being transmitted to the intended recipients in due time;
- Potential distrust of the Member States in the ECRIS communication network;
- Degradations in the performance of the local national servers and/or communication networks;
- Inaccessibility of the ECRIS system and of its functions.

1.8.4 *Lack of "Non-Repudiation" Controls*

Two types of non-repudiation controls must be considered in the frame of ECRIS.

The first concern the *non-repudiation of origin* which aims at assuring that the original sender of information cannot successfully deny that a given request was sent. The second concern the *non-repudiation of receipt* which aims at assuring that the sender of information is protected against the denial of the receiver, who may claim that the sender never sent the information, or that he did not send it on time. The consequences that could happen due to missing controls are:

- Violation of the ECRIS legal basis (LEG_01, LEG_03);
- Requests and responses to requests not being transmitted to the intended recipients in due time;
- No respect of the "Need to Know" concept.

1.9 Threats and Vulnerabilities

The threats used and identified in this study originate from the EBIOS 2010 Knowledge Base Catalogue. Please note that only the threats that are relevant to ECRIS due to the decentralised nature of the system and of the message exchanges were considered.

"ANNEX I" lists all threats of the EBIOS Knowledge Base [5] and identifies the ones that are applicable in the context of the ECRIS security analysis. The table below lists these threats that can potentially affect ECRIS and identify for each such threat the vulnerabilities of the system. Please note that the "EBIOS ID" refers to the threat identifier of the EBIOS Knowledge Base. The vulnerabilities are the weaknesses in the system as a whole (i.e. not only the IT software application but all the components of the system) which could be used by potential attackers for breaking the security qualities defined earlier.

EBIOS ID	THREATS	VULNERABILITIES
M7	**Misuse of software system** The system is used to perform actions other than those intended. Examples: § The system is used to gather information on convictions of a citizen outside the legal framework (e.g. curiosity, corruption…). § The system is used to send information that is not in the scope of the legal framework (e.g. sending of illicit attachments).	§ End users able to send requests are spread in all the Member States. They are under the responsibility of central authorities of the Member States. There is no centralised access control or monitoring service. § Systems to access ECRIS are spread in all the Member States. They are under the responsibility of central authorities of each Member State. There is no centralised access control or monitoring service. § Presence of attachments in the payload of messages being transmitted.
M9	**Exceeding the limits of software system**. The processing capability of the information is exceeded, or the software is malfunctioning due to malformed input data. Examples: § Too many requests to handle. § Buffer overflow.	§ No limits on the number of requests that can be sent within a certain time frame. § Presence of attachments in the payload of messages being transmitted. § No limit on the number and size of the attachments that can be included in the payload of messages being transmitted.

M11	**Changes to the software system** Inappropriate handling during the update, configuration or maintenance (Enable or disable of features, change in network settings or routing rules, modification or addition of features, malicious code). Examples: § Unexpected change in the payload format. § Unexpected change of an IP address of a server. § Presence of malicious code in an attachment.	§ Changes in the format of the payload of messages being transmitted. § Changes in the network configuration of a Member State. § Presence of attachments of the payload.
M13	**Man-in-the-middle attack on a data channel or telephone connection** Eavesdropping on the communication network and/or loss of communication integrity by taking control of the connection. Example : § This can occur on the national network if network encryption is not implemented.	§ Exchange of information on a shared communication network (sTESTA and national networks). § Lack of best practice policy regarding the use of security certificates.
M14	**Passive listening on a data channel or telephone connection** Acquisition of data by eavesdropping on the network. Examples : § Sniffing of the network traffic (e.g. port mirroring). § Packet tracing on network devices. § Access to the clear text segment of the TAP by the sTESTA administrators if end-to-end encryption is not enforced (e.g. HTTPS).	§ Exchange of information as clear text on parts of the communication network.
M15	**Saturation of a data channel or telephone connection** The flow of information can be slowed down or even blocked. Overuse of network bandwidth. Examples : § Usage of the maximum bandwidth of the sTESTA connection. § Usage of the maximum bandwidth of a segment of the national networks.	§ Under-sizing of the bandwidth of the communication network. § No limits on the number and sizes of the attachments that can be included in the payload.

M19	**Inappropriate assignment of activities to a person (resulting in unintended action of a user)** Example : § Misrouting of a request to a Member State for which it was not intended (misrouting) due to a wrong operation of the user.	§ There is no systematic implementation of control measures in all Member States to cross-check the routing of the information to the right destination. § There is no systematic implementation of logging of operations in all Member States.
M23	**Influence on a person** Person that can be forced or required to disclose or modify data. Examples : § Corruption § Curiosity	§ Users able to send requests are spread in all the Member States. They are under the responsibility of central authorities of the Member States. There is no centralised access control or monitoring service. § Systems to access ECRIS are spread in all the Member States. They are under the responsibility of central authorities of the Member States. There is no centralised access control or monitoring service.

Table 2 – Identification of system vulnerabilities

1.10 Risk Matrix

This section identifies the risks, based on the previous definitions of the required security qualities and identified vulnerabilities of ECRIS as a system. For each risk, the probability of occurrence and gravity of the impact is estimated in order to be able to classify the risks by their importance.

The risk matrix below provides the following:

§ A unique identifier for the risk

§ The threat as defined in EBIOS

§ The estimated gravity of the impact on ECRIS if the threat would occur:

– H = High (associated numeric value = 3)

– M = Medium (associated numeric value = 2)

– L = Low (associated numeric value = 1)

The estimation of the impact is purely subjective, based on the knowledge of iLICONN at the time of writing of this document, and should be further discussed with the different stakeholders of ECRIS.

- The estimated probability that a threat occurs:
  - H = High (associated numeric value = 3)
  - M = Medium (associated numeric value = 2)
  - L = Low (associated numeric value = 1)

  The estimation of the probability of occurrence is purely subjective, based on the knowledge of iLICONN at the time of writing of this document, and should be further discussed with the different stakeholders of ECRIS. The factors to be taken into account are varied, such as the number of potential occurrences or the feasibility of the threat.

- The risk exposure is a value attributed to the risk for the purposes of comparing the importance of the risks and it is calculated as follows: risk exposure = probability x impact. The risk exposure is rated as:
  - High if it is higher or equal to 5,
  - Medium if it is 3 or 4 and
  - Low if it is 1 or 2 as depicted in the following table:

Probability / Impact	L(1)	M(2)	H(3)
L(1)	L (1)	L (2)	M (3)
M(2)	L (2)	M (4)	H (6)
H(3)	M (3)	H (6)	H (9)

Table 3 – Risk exposure table

§ The security qualities being affected:

- C = Confidentiality
- I = Integrity
- A = Availability
- NRO = Non-repudiation of Origin
- NRR = Non-Repudiation of Receipt

ID	Threat	Risk Exposure	Impact	Probability	Impact on Security Qualities				
					C	I	A	NRO	NRR
R1	[M7] Misuse of software system	H (6)	H	M	X	X	X	X	X
R2	[M9] Exceeding the limits of software system	M (4)	M	M			X		
R3	[M11] Changes to the software system	H (6)	H	M	X	X	X	X	X
R4	[M13] Man-in-the-middle attack on a data channel or telephone connection	M (3)	H	L	X	X			
R5	[M14] Passive listening on a data channel or telephone connection	H (6)	H	M	X				
R6	[M15] Saturation of a data channel or telephone connection	L (1)	L	L			X		
R7	[M19] Inappropriate assignment of activities to a person (resulting in unintended action of a user)	L (2)	L	M	X			X	X
R8	[M23] Influence on a person	M (3)	H	L	X	X		X	X

Table 4 – Risk matrix

1.11 Risk Mitigation Measures

This section identifies the possible measures that can be taken for mitigating the risks identified above. These measures aim at reducing the probability of occurrence and/or the gravity of the impact of the targeted risk. Please note that at this stage, the measures can be of different natures such as procedural, organisational, technical, environmental or related to the infrastructure of the system. Please note that for identifying suitable measures for ECRIS, the authors took into consideration the following:

1. The security measures currently implemented in NJR;
2. The EBIOS Methodology [5];
3. The DIN ISO/IEC 27002:2008-09 [19] standard.

In the context of ECRIS, the focus is to be put on the following mitigation measures:

[C1] Test of the availability of the Member States' ECRIS sites and applications

This measure aims at minimising the possibility of failing to adhere to the service availability requirements by pro-actively monitoring the availability of the network and national services and taking corrective measure when an availability issue is identified.

[C2] Logging of the operations

This measure is based on the systematic logging of all operations performed by the ECRIS applications. This can be used preventively against misuse of the national systems and as a measure to support *Non-repudiation of Origin* and *Non-repudiation of Receipt*[1] and ensure the traceability of all operations performed in ECRIS.

[C3] Signature of the request

This measure is based on the digital signature of the "request" messages issued by the requesting Member States central authority so as to ensure *Non-Repudiation of Origin*. The possession of a request that has been signed by a given sender serves as a proof that the request was indeed sent by the entity to which the digital signature belongs. In addition, digital signatures can be used to authenticate the sender and ensure the integrity of the requests.

[1] It is assumed that the national servers are trusted to keep logs as specified. In the framework of ECRIS this is valid assumption on the grounds that the Member States are trusted to put in place all the necessary measures to ensure that their servers are not acting in a malicious way.

[C4] Sending of an automatic signed acknowledge message

This measure is based on the sending of an automatic, digitally signed, acknowledgment message by the requested Member States' central authority ECRIS application, confirming to the requesting Member State the proper receipt of the "request" message so as to ensure *Non-Repudiation of Receipt*[2]. As the information exchange in ECRIS occurs between two servers and not two users, non-repudiation could only be implemented at national level and not on end user level. In any case, this measure could help during investigation related to the misusing of the system. Such a signed acknowledgment could serve as strong evidence that a message has indeed been received by the intended recipient to which the signature belongs.

[C5] Retransmission process

A retransmission process can be supported by defining appropriate kinematics, rules and policies defining how, when and how often the ECRIS applications should retry the transmission the same XML messages after a failure. This can serve as a mitigation measure for minimising the impact of service unavailability.

[C6] Encryption of data

Encryption of the criminal records information during their transmission can be used to ensure the confidentiality of the information. Despite the fact that data is already encrypted on the sTESTA network, there is a need to enforce encryption between the local site of the Member State and the sTESTA national access point. It is noted that encryption of the transmitted information is also a technical requirement implied by the ECRIS legal basis (LEG_O4). This requirement can only be fulfilled by implementing an end-to-end encryption solution; i.e. the data needs to be encrypted at the server of the transmitting central authority and be decrypted at the server of the receiving central authority.

Please note that the use of HTTPS meets well this requirement as it offers a sufficient level of protection, provided that it is implemented in accordance with the HTTPS specification and that up-to-date best practices regarding cipher suites and handling of the HTTPS security certificates are observed.

[2] On the assumption that the server that acts as receiver is trusted to send the acknowledgment upon receipt of a request. In the framework of ECRIS this is valid assumption on the grounds that the Member States are trusted to put in place all the necessary measure to ensure that their servers are not acting in a malicious way.

[C7] Procedure for configuration changes (versioning)

This measure is of organisational nature and is based on the clear definition of procedures for properly managing and controlling changes that are to be performed on the various components that constitute ECRIS as well as on the elements that are used to run and operate the ECRIS implementations.

This measure can be implemented by combining several elements:

- The definition of a proper versioning mechanism for the technical artefacts of the ECRIS applications.
- The definition of procedures allowing the configuration changes to be communicated between all ECRIS stakeholders so that the appropriate actions can be taken for avoiding disruption of the service. This part is organisational and thus out of scope of the *ECRIS Technical Specifications* project.

[C8] Set-up of an ECRIS central PoC

This measure is of organisational nature and is based on the definition of a central “Point of Contact” for ECRIS that coordinates and communicates on a regular basis on ECRIS-related matters and evolutions to all stakeholders.

This measure can mitigate various operational risks arising from changes at organisational and technical level as well as mitigating the risk of service ~~availability~~ unavailability.

[C9] Capacity planning

This measure is based on the definition of the maximum amount of messages and maximum volume of data that ECRIS is capable of completing in a given time period, as well as the regular monitoring on the usage of the resources necessary to complete the processing of such messages.

Capacity planning can be used as a measure to mitigate risks R2 and R6 that may affect the availability of the service.

[C10] Policy for the use of attachments

This measure is based on the definition of a policy that governs the use of binary attachments linked to the ECRIS messages so as to keep control in particular on the nature and on the content of these binary files.

A policy that governs the use of the attachments can mitigate risks R1 and R2 that may affect the availability of the service.

[C11] Memorandum of Understanding (MoU)

The overall security degree of ECRIS depends not only on the measures implemented at the level of information exchange and technical communication services that are in the scope of this document but also on the security of the national systems. To that extent, there are many aspects of security that lie within the responsibility of the Member States' central authorities. This measure is based on the definitions of a Memorandum of Understanding on security aspects, to be agreed among all Member States in order to define best practices and standards that should be followed by all Members States so as to ensure a minimum common level of security.

[C12] Routing ACL

This measure is based on the definition of appropriate filtering and access lists at network level so as to block unauthorised access and thus to strengthen the protection against various attacks that could compromise the security of data and the national systems.

[C13] Authentication of the communicating parties

This measure is based on the usage of technical mechanisms allowing the unique authentication of the authorities communicating via ECRIS.

In the context of ECRIS, authentication can only occur between the servers of the central authorities participating in the exchange of information. Two types of authentication can further be identified:

a) **One-way authentication** (aka simple authentication) where the sender authenticates the receiver to ensure that the information is sent to the correct server. In this case the sender can ensure that the information is not send to the wrong server, but the receiver cannot verify the identity of the sender at the time the information arrives.

b) **Mutual authentication** where both communicating servers authenticate each other to ensure that the information is sent to the correct server and that the information received has been sent by the claimed server. Mutual authentication, if used correctly, can be used also as excellent protection against "man-in-the-middle" type of attacks.

It is noted that one-way authentication is a prerequisite for establishing secure communication channels. There is a wide range of authentication protocols. In the framework of ECRIS a realistic solution is to use HTTPS and certificates for one-way authentication. Mutual authentication can be implemented by the use of two-way SSL.

[C14] Use of cryptographic techniques to verify the integrity of the received data

This measure relies on the usage of digital cryptographic techniques that can be used to verify the integrity of the data. Typically, secure hash functions are used quite often for the verification of integrity. This technique is supported by HTTPS. SSL calculates the digest of the message and appends that digest to the encrypted data.

The mitigation matrix lists all proposed measures along with the following information:

§ The unique identifier of the measure;
§ The type of measure;
§ The risks and security needs covered by the measure, using the references established in the previous chapters;
§ The organisation entity that is responsible for implementing the measure.

ID	Measure	Risks / needs covered	Responsibility
C1	Test of the availability of the Member States' ECRIS sites and applications	LEG_02 R1, R2, R3, R6	ECRIS central PoC (Point Of Contact)
C2	Logging of the operations	LEG_01, LEG_03 R1, R7, R8	Member States ECRIS central PoC
C3	Signature of the request	LEG_03 R1, R4, R8	Member States
C4	Sending of an automatic signed acknowledge message	LEG_01	Member States
C5	Retransmission process	LEG_02	Member States
C6	Use of encryption	LEG_04 R4, R5	Member States
C7	Procedure for configuration changes (versioning)	LEG_02 R3	Member States ECRIS central PoC
C8	Set up of an ECRIS central PoC	LEG_02 R3	ECRIS central PoC
C9	Capacity planning	LEG_02 R2, R6	Member States ECRIS central PoC
C10	Policy for the use of attachments	LEG_02 R1, R2	Member States

C11	Memorandum Of Understanding (MoU)	All	Member States
C12	Routing ACL	LEG_04 R4, R5	Member States
C13.a	One-way authentication	LEG_01, LEG_04 R5	Member States (ECRIS central PoC depending on how certificates are exchanged)
C13.b	Mutual authentication	LEG_01, LEG_02, LEG_03, LEG_04 R4, R5	Member States (ECRIS central PoC depending on how certificates are exchanged)
C14	Use of cryptographic techniques to verify the integrity of the received data.	LEG_04 R4	Member States

Table 5 – Risk mitigation measures

The following table depicts which legal requirements and risks are addressed by each proposed measure. It is to be noted that each legal requirement and risk is addressed by at least two different measures.

Measure ID	LEG_01	LEG_02	LEG_03	LEG_04	R1	R2	R3	R4	R5	R6	R7	R8
C1		X			X	X	X			X		
C2	X		X		X						X	X
C3			X		X			X				X
C4	X											
C5		X										
C6				X				X	X			
C7		X					X					
C8		X					X					
C9		X				X				X		
C10		X			X	X						
C11	X	X	X	X	X	X	X	X	X	X	X	X
C12				X				X	X			
C13.a	X			X					X			
C13.b	X	X	X	X				X	X			
C14				X				X				

Table 6 – Proposed measures addressing legal requirements and identified risks

1.12 Possibilities for Implementing Risk Mitigation Measures

The following sections elaborate on the possible techniques that are available in the context of ECRIS for implementing the mitigation measures described in the previous chapter.

In view of identifying appropriate security techniques for ECRIS, the authors have based themselves on their experience in security and took into consideration, among others, the sources [12] – [18] listed in section §1.3.

Please note that some of the measures identified and described in the following sections are not necessarily in the scope of the *ECRIS Technical Specifications* project. Although these are briefly outlined here for the sake of completeness, it is not the aim of the *ECRIS Technical Specifications* to actually implement them.

1.12.1 *Testing of Availability of Member States' Sites from Central Point (C1)*

This technique implements the mitigation measure "[C1] - test of the availability of the Member States' ECRIS sites and applications".

The tests on the availability of the *web services* running on the servers of all the Member States' central authorities are performed from a central site. This is used for statistics purposes as well as for the trouble-shooting of connectivity problems. Such tests can either be performed pro-actively on a regular basis so as to have automatic monitoring of the availability of the systems or using ad-hoc procedures triggered manually upon request.

Such testing facility could be under the responsibility of a centralised ECRIS Point of Contact and a specific tool should be developed for this purpose. Please note that testing with ICMP (ping) should be avoided as it will mostly be denied by security devices and/or national networks. Such a centralised tool should rather use a specific *web service* defined at the level of the ECRIS applications.

1.12.2 *Decentralised Testing of Availability of Member States' Sites (C1)*

This technique also implements the mitigation measure "[C1] - Test of the availability of the Member States' ECRIS sites and applications".

The tests on the availability of the *web services* running on the servers of all the Member States' central authorities are performed between all Member State's ECRIS applications by using *web services* specifically designed for this purpose.

1.12.3 *Decentralised Logging of Operations (C2)*

This technique implements the mitigation measure "[C2] - Logging of the operations".

Logging of all operations performed by the end-users and administrators in the Member States central authorities can only be performed locally in the Member States since no information is centrally stored. In any case, a procedure needs to be established and agreed by all stakeholders of ECRIS for analysing the different logging information in case of suspected misuse of ECRIS or corruption.

In addition, Member States should synchronise their logging timestamps, for example by using NTP (Network Time Protocol).

1.12.4 WS-Security *(C3, C4, C6, C13.b, C14)*

1.1.1.1. Introduction

As defined in more details in the document "Technical Architecture", ECRIS is a completely decentralised information exchange system between the central authorities of the Member States. Also, the protocols and standards that are defined for realising the data exchanges are based on the usage of *web services* and *SOAP*.

Within this context, the *WS-Security* specification, which is an extension to the *web services* specification, can be considered since it proposes a standardised way to implement all the cryptographic controls that are proposed as mitigation measures, namely:

- [C3] – Signature of requests;
- [C4] – Sending of an automatic signed acknowledge message;
- [C6] – Encryption of data;
- [C13.b] – Mutual authentication;
- [C14] - Use of cryptographic techniques to verify the integrity of the received data.

WS-Security proposes a complete set of mechanisms that allow *SOAP* message signing, encryption and attachment of security tokens. Additionally, the specification supports various signature formats, encryptions algorithms and multiple trust domains, and is open to various security token models, such as *X.509* certificates, *Kerberos* tickets and combinations of username/password credentials or custom defined tokens.

WS-Security is a building block that can be used in conjunction with other *web service* extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies. In essence, *WS-Security* ~~combines~~ defines the use of *XML-Signature* and *XML-Encryption* in SOAP headers so as to achieve the required security ~~functionality~~ (please refer to [15]).

Please note, however, that *WS-Security* by itself does not provide any guarantee of security. When implementing and using the framework and syntax, it is up to the implementer to ensure that the result is not vulnerable to attacks. It thus requires specific security-related experience in order to be implemented properly.

The main benefit of using *WS-Security* is the fact that it is a specification created for *web services*, designed specifically for implementing security features such as encryption or message signing. It is mature and well accepted within the *web services* community and well supported by different vendors.

There are, however, a few particularities of *WS-Security* that should be taken into account:

- Depending on the technical platforms used by the *web service* implementers, the usage of *WS-Security* can occasionally give rise to interoperability issues. This depends on the *WS-Security* components that are actually used. As an example, according to the interoperability guidelines issued by Oracle, asymmetric binding for *WS-Security* 1.1 is not guaranteed for the .NET Framework (please refer to [11]).
- Depending on the implementation of the encryption and of the message signature chosen, potential performance overheads can occur. Please note that, in general, an impact on performance is always to be expected when using cryptography. When *WS-Security* is used, the impact may be higher mainly due to repeated cryptographic operations on XML message parts and notably due to XML canonicalization.

1.1.1.2. Consideration on encryption of data

WS-Security allows for encryption of the messages exchanged so as to avoid transmitting sensitive data in clear text, which would be against legal requirements LEG_04.a (data confidentiality) and LEG_04.c (use of encryption). In order to implement appropriate encryption, an additional task is required for defining and agreeing precisely on the level of encryption to be reached, that is on the encryption algorithms and key sizes to be used.

In doing so, it is important that the impact of the cryptographic operations on performance is taken into consideration. In the case of *WS-Security*, the impact of XML canonicalization on performance and size of the messages should also be considered.

1.1.1.3. Sending of automatic signed acknowledge message (C4)

In regards to *Non-Repudiation of Receipt*, an acknowledgment message can be signed and returned to each request by using *WS-Security* so as to ensure that it was received and acknowledged by the receiver. In respect to the level of security offered, this solution is the most appropriate, since the response message is irrefutably signed by the receiver in a way that cannot be counterfeited except if the security of the receiving server is compromised.

1.1.1.4. Alternative

Please note that an alternative could be the usage of the *WS-SecureConversation* extension to the *web services* specification. The main purpose of *WS-SecureConversation* is to establish security contexts for multiple *SOAP* message exchanges, reducing significantly the processing overhead of key establishment when compared to *WS-Security* in the case of frequent message exchanges. However in practice *WS-SecureConversation* is a layer put on top of *WS-Security* which has additional dependencies to other WS-* protocols like *WS-Addressing* and *WS-Trust*. The gain in processing is counterbalanced by added complexity and an increase of the risk of interoperability issues.

1.12.5 *Adding Explicit Unsigned ACK Messages in Kinematics (C4)*

This technique implements partly the mitigation measure “[C4] - Sending of an automatic signed acknowledge message”.

In the NJR pilot project, an approach is already followed for returning systematically and automatically an acknowledgment message in order to inform the sender of the successful receipt of a message. This message is an additional synchronous *web service* operation and is not electronically signed.

The advantage of this approach compared to *WS-Security* is obviously its simplicity. Furthermore, since the message is unsigned, it is less heavy in terms of processing required given that the asymmetric cryptographic algorithms used for signing messages are quite processor-intensive.

The main drawback is that the mitigation measure is only implemented partially. In particular, there is no way to verify technically that the acknowledgment message is valid and irrefutably transmitted by the receiver. Please note that this drawback can be tackled by the usage of cryptographic signatures.

1.12.6 *Using* SOAP *Return Code as Automatic ACK Message (C4)*

This technique implements partially the mitigation measure "[C4] - Sending of an automatic signed acknowledge message".

As also described in the document "Technical Architecture", Chapter 3.3.2 - Error types and error handling", p. 15, paragraph 2, any request is considered to be properly received as soon as the receiving server replies with the HTTP "Status 200" code which, as per the *RFC216* upon which *SOAP* is based for HTTP bindings, translates as "Success - The action was successfully received, understood, and accepted". In case the request is not properly received, understood and accepted, then the return message will be a "SOAP Fault" exception (or of a custom type extending the "SOAP Fault" exception and specifically designed so as to express a specific erroneous situation).

Indeed, as per SOAP 1.2 specification and more specifically on "SOAP version 1.2 Part 2: Adjuncts", chapter "7.5.1.2 Requesting", which are part of the proposed specifications that should be adopted by all Member States, a clear association is created between the different HTTP Status codes and the SOAP execution states. Based on this, if the HTTP return code is not 4xx (client errors) or 5xx (internal server errors), the message must be considered as well-received. This of course does not imply that the message is functionally valid, but in the context of ECRIS, this validation happens asynchronously and is supported by separate kinematics.

The main advantage is that this solution is even easier than explicitly defining and sending ACK messages while achieving the same goal since the HTTP 200 status can be considered as an acknowledgement from the receiver that the message was received.

The drawback is mainly that the mitigation measure is only implemented partially. In particular, there is no way to verify technically that the acknowledgment message is irrefutably transmitted by the receiver.

1.12.7 *HTTPS with One-Way Authentication (C6, C13.a, C14)*

This technique implements the mitigation measures:

- "[C6] - Encryption of Data"
- "[C13.a] – One-way authentication"
- "[C14] - Use of cryptographic techniques to verify the integrity of the received data"

The use of HTTPS with one-way authentication (aka simple authentication) is considered to be a viable solution for establishing a secure encrypted communication channel at the level of the ECRIS applications. Please note also that this mechanism is already used in the NJR pilot project and is considered secure by all Member States participating in NJR.

HTTPS is a combination of HTTP with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. The main idea of HTTPS is to create a secure channel over a potentially insecure network. This ensures reasonable protection from eavesdroppers, provided that adequate *cipher suites* are used and that the server certificate is verified and trusted by the client. More concretely, to consider HTTPS with simple authentication secure, the following statements must be true:

1. The HTTP client software correctly implements HTTPS and has a valid and up to date registry of certificate authorities.
2. A certificate authority that is considered valid and trusted from the HTTP client software vouches for the legitimacy of the certificate provided.
3. The certificate is valid and correctly identifies the site or entity using it.
4. The cryptographic suite used is considered sufficiently trustworthy.

While the solution of HTTPS using simple authentication is fairly simple to set-up, it is known not to be fully secure against "man-in-the-middle" attacks.

1.12.8 *HTTPS with Mutual Authentication (C6, C13.b, C14)*

This technique implements the mitigation measures:

- "[C6] - Encryption of Data"
- "[C13.b] – Mutual authentication"
- "[C14] - Use of cryptographic techniques to verify the integrity of the received data"

This technique is an extension of the "HTTPS with One-Way Authentication" method described earlier. This variation of HTTPS is considered more secure since both the server and the client must use secure certificates in order to properly authenticate each other. The main advantage is that it provides maximum security because, in addition to establishing a secure encrypted communication channel, it allows the receiver to authenticate the origin of the incoming data.

However this technique is known to be difficult to set-up, as it requires specific configurations in the network layer in case of reverse proxies or similar network elements are used and thus can add a significant overhead for reaching proper connectivity between Member States.

1.12.9 *Custom Digital Cryptographic Signatures (C3, C4, C13.b)*

This technique implements the mitigation measures:

- "[C3] – Signature of requests"
- "[C13.b] – Mutual authentication"

It also provides a part of the implementation for "[C4] - Sending of an automatic signed acknowledge message".

It is possible to establish custom digital signature of the XML messages being exchanged between the Member States' central authorities by using a hash function and encrypting/decrypting the output checksum using asymmetric key cryptography algorithms (i.e. private and public keys).

This document does not elaborate on the detailed specifications of such a solution but lists it for the sake of completeness.

While it provides an implementation for security qualities such as *non-repudiation of origin* and *non-repudiation of receipt*, it adds a high level of complexity for implementing the ECRIS applications and is not a preferred approach.

1.12.10 *Definition of Central Body (C8)*

As mentioned already in the "Inception Report" document, the definition of a central body taking care of the coordination of changes also implements mitigation measure "[C8] – Set-up of an ECRIS Central PoC".

Such a central body would act as a service desk, consolidate and communicate all information regarding organisational and/or technical changes (e.g. contact list, IP addresses, etc.). The information could be made available to the designated Member States staff on a protected area of the sTESTA portal.

The following activities could be supported by such an organisation:

- Information consolidation on the system configuration of all Member States (e.g. server's certificate management and distribution).
- Documentation management
- 2nd level support
- Change management
- Incident reporting (technical incidents, security incidents)
- Contact list management
- Statistics
- Directory of digital certificates

Please note that establishing such a central body as well as the detailed description of its mission is crucial for implementing ECRIS but is out of scope of the *ECRIS Technical Specifications* project.

1.12.11 *Establishing Limits in Message Exchanges (C9)*

This technique implements the mitigation measure "[C9] – Capacity planning".

In order to avoid saturating the communication channels, in particular the network nodes and ECRIS applications, limits on the maximum number and volume of the messages that can be sent within a certain time frame by the Member States' central authorities using ECRIS are defined and implemented into the software systems.

1.12.12 *Network Bandwidth Monitoring (C9)*

This technique implements the mitigation measure "[C9] – Capacity planning".

During the operational usage of ECRIS after April 2012, the sTESTA network provider as well as the national network providers should pro-actively monitor the bandwidth usage of ECRIS and provide the Member States and/or the ECRIS Central PoC with detailed reports so as to avoid any performance problems on the communication lines.

1.12.13 *Establishing Limits in Use of Attachments (C10)*

This technique implements the mitigation measure "[C10] – Policy for the use of attachments".

In order to limit the number of threats related to the usage of binary attachments, a technical policy is established for limiting:

- The authorised types for the attachments;
- The maximum size for each attachment and of the total of all attachments;
- The maximum number of attachments per message.

Please note however that the content checking of the attachments, and in particular making sure that the attachments are free from viruses or malware, is an important element for successfully implementing this mitigation measure but it lies within the responsibility of the Member States' central authorities and is therefore not dealt with in the *ECRIS Technical Specifications* project.

1.12.14 *Memorandum of Understanding (C11)*

As indicated in the "Inception Report", since ECRIS is conceived as a decentralised system, many aspects of security of the system lie within the responsibility of the Member States' central authorities.

It is therefore proposed that a Memorandum of Understanding (MoU) is defined, agreed upon and signed by all Member States. This document should define best practices and standards to be followed and ensure that the Members States are compliant with a minimum common level of security by providing best practices, policies and guidelines on topics such as:

§ Perimeter security;

§ End-user awareness and clearance;

§ Internal IT infrastructure of the Member State's criminal records registers (i.e. criminal records databases or mainframes, national and local networks, desktops of the central authorities' personnel, national and local servers, etc.);

§ The measures for protecting the accesses to the criminal records register or ECRIS application from within a Member State's central authority;

§ Protection of personal data;

§ *Etc.*

Please note that implementing this mitigation measure, and in particular drafting the MoU, is clearly out of scope of the *ECRIS Technical Specifications* project.

1.12.15 *Routing ACL (C12)*

Appropriate filtering and access lists are implemented in the network layer to mitigate the risk of unauthorised access to ECRIS server instances and to limit the exchange of ECRIS information only between authorised servers. This can be realised for instance by configuring ACL (Access Control Lists) on the national access points to sTESTA, or LNI (Local National Interface) (e.g. router or firewall of the Member State).

Conclusions

The present document has identified a number of security risks and possible concrete measures that can be implemented for mitigating them.

Based on the responses of the Member States to the “Inception Phase Questionnaire”, the feedback received during the visits to five Member States, the current NJR practice, as well as the results of the Expert Subgroup meeting that took place on 22 September 2010, the list of measures identified below are reflecting the balance between the efforts to be provided for implementing these mitigation measures and the risks accepted by the Member States.

1.12.16 *Implemented Mitigation Techniques*

Considering the facts that:

- The ECRIS technical specifications must comply with the ECRIS legal basis;
- ECRIS should remain as close as possible to the NJR pilot project;
- The implementation work should be kept simple so as to not jeopardise the timely development of the ECRIS applications;
- The ECRIS applications should be sufficiently secure so as to at least address the highest priority risks;
- Each Member State must be able to freely implement routing rules and network policies, independently of the ECRIS technical specifications, for establishing the connections between the ECRIS server of its central authority and the sTESTA network itself.

The following mitigation techniques are to be implemented for the first version of the ECRIS applications and taken into account in the definition of the ECRIS technical specifications:

a) Decentralised Testing of Availability of Member States’ Sites (C1)

In the first version of ECRIS, a simple monitoring of the availability of the Member States’ ECRIS applications is to be performed.

The document “Technical Architecture” describes the definition of an “isAlive” *web service* that allows any ECRIS implementation to verify whether the target host can be reached (i.e. verification that connectivity is established) and whether the target host is able to respond to calls.

b) Decentralised Logging of Operations (C2)
The *ECRIS Technical Specifications* project foresees already the delivery of the "Logging, Monitoring and Statistics Analysis" document. This document establishes the procedures for logging the operations performed by the ECRIS applications and for monitoring their functioning.

c) Using *SOAP* Return Code as Automatic ACK Message (C4)
This is covered already by the document "Technical Architecture" which describes the usage of the synchronous return of the *web service* calls in order to determine whether a message was successfully received (i.e. HTTP return code 200) or whether an error of technical nature occurred. The proper return of the synchronous *web service* call is to be understood as confirmation to the requesting Member State that the "request" message was properly received without technical errors by the requested Member State.
Please note that in addition, if no functional errors are returned asynchronously as described in the document "Technical Architecture", then it can also be considered that the "request" message was properly received without functional errors by the requested Member State.

d) Retransmission process (C5)
The "Detailed Technical Specifications" documents need to define the necessary technical kinematics for ensuring proper handling of technical errors and need to describe how, when and how often the ECRIS applications must/should retry the transmission of the same XML messages after a failure.

e) HTTPS with One-Way Authentication (C6, C13.a, C14)
HTTPS encryption with one-way authentication using only server-side HTTPS security certificates is to be implemented in the first version of the ECRIS applications. The specific details for this implementation are provided in the next section.
It is noted that since one-way authentication does not authenticate the sender, the integrity of an incoming message cannot be verified the moment the message is received (i.e. it cannot be verified that the received message has been sent by the claimed sender). This problem can be partially alleviated via subsequent exchanges of messages as it is currently the case in NJR. A higher degree of security can be reached in later versions of ECRIS, relying on encryption of the data and mutual authentication. The recommended techniques to be investigated later are either "HTTPS with mutual authentication" or "*WS-Security*".

f) Configuration management – Versioning (C7)
This is covered already partly by the document "Technical Architecture" which describes the versioning principles to be implemented in ECRIS for supporting subsequent versions of the ECRIS technical specifications.
Please note that the definition of procedures allowing the configuration changes to be coordinated and communicated between all ECRIS stakeholders, so that the appropriate actions can be taken for avoiding disruption of the service, is an organisational matter which needs to be handled by the Member States. This part is out of scope of the *ECRIS Technical Specifications* project. However this analysis recommends describing and setting up a central body, probably under the hood of an EU institution, which should fulfil these organisational coordination and communication tasks.

g) Establishing Limits in Message Exchanges (C9)
The "Detailed Technical Specifications" documents need to define the necessary limitations in terms of the maximum number and volume of the messages that can be sent within a certain time frame using ECRIS.

h) Establishing Limits in Use of Attachments (C10)
The "Technical Architecture" document defines the limitations in terms of types of binary files that can be attached to the ECRIS XML messages as well as the total size of such XML messages (including the binary attachments).

The following mitigation techniques should be implemented by April 2012 (not in scope of the *ECRIS Technical Specifications* project):

i) Definition of Central Body (C8)
j) Routing ACL (C12)

1.12.17 *HTTPS Certificate Specifications*

In the context of ECRIS, and given the statements mentioned above for HTTPS to be considered secure, the following recommendations must be followed for implementing HTTPS with one-way authentication.

1.1.1.5. Management of HTTPS certificates

Regarding the HTTPS server certificate, each central authority may acquire it from any valid certification authority of its choice that is trusted either by all or by the specific central authority, or issue a self-signed certificate meeting the requirements elaborated in this chapter. All Member States agree to trust each other's public certificates.

The follow-up, coordination and communication tasks are to be performed by a central body that needs to be defined and set-up for this purpose after the *ECRIS Technical Specifications* project. Once a Member State's central authority has acquired a new certificate, it exports the server's public certificates in an acceptable format, such as PEM, and provides these to the central body over a trusted, preferably off-line, communication channel that guarantees the integrity of the certificates. This central entity is then responsible for publishing the public HTTPS security certificates and making them available through secure channels to the Member States' central authorities. This central entity must also perform coordination and follow-up, such as for example informing the Member States' central authorities of expirations of certificates, extensions of the validity of certificates, future replacements of certificates, etc.

The Member States' central authorities take all appropriate technical actions so as to fetch the public certificates and to install them in the local trusted certificate store which is used by the HTTP client software of the national ECRIS implementations. This is required so that the HTTP client can actually validate the certificates received during the runtime execution of the ECRIS applications.

Please note also that, in order to avoid temporary loss of service, the HTTPS server certificates must always be renewed before reaching their expiration date.

1.1.1.6. Technical Recommendations

Regarding the SSL implementation between clients and servers, the use of SSL 2.0 is to be prohibited due to known serious vulnerabilities. The communication protocols to be considered for the deployment of transport layer security are SSL 3.0 or TLS 1.2. Please note here that the two protocols carry significant differences between them and thus cannot be considered interoperable. However, TLS 1.2 incorporates mechanisms allowing the negotiation with SSL 3.0.

The parameters of the “*Cipher Suite*” must at least comply with the following recommendations:

- Key establishment: Use of DHE (Diffie-Hellman Ephemeral) or RSA.
- Confidentiality: Use of AES 128 or better 256 bit keys.
- Signature: Use of RSA algorithm and private leys of minimum1024bits.
- Hash: Use of SHA-1 algorithm or better SHA-256 as SHA-1 is vulnerable to collisions.

The RSA private keys must have a length of at least 1024 bits, with 2048 bits recommended as it is estimated that 1024-bit keys will become easy to compromise in the near future. The validity period of the certificate must not exceed **24 months**. Moreover, the following information is to be used for create the certificate:

- Country Name: the two letter ISO 3166-1-alpha-2 code of the Member State;
- State or Province name: the state or province (whichever applicable) in which the Member State’s central authority is located;
- Locality: the name of the city in which the Member State’s central authority is located;
- Organisation Name: the name of the parent organisational to which the Member State’s central authority belongs to;
- Organisational Unit Name: the name of the Member State’s central authority;
- Common name: the domain name of the ECRIS server instance that will be used;
- Email address: the e-mail address of the webmaster being responsible for the ECRIS server instance identified by “common name”.

The HTTP client software component used by the national ECRIS implementations must provide a proper HTTPS implementation, especially in regard to properly identifying a server, as described in RFC 2818 chapter “§3.1 Server Identity” (please refer to http://www.ietf.org/rfc/rfc2818.txt for more detailed information).

More specifically, the following checks must be performed by the HTTP client software when receiving a server certificate during the runtime execution of ECRIS:

- Verifying the validity of the certificate chain.
- Verifying that the certificate has not yet expired (i.e. compare expiration date of certificate with current date)
- Verifying that the information provided in the certificate is valid and matches the information provided in the locally stored certificate that has previously been exchanged using an out-of-band secure channel.

Even though it is beyond the scope of this document to provide specific security policies and measures on the Member States IT assets, the following recommendations should be taken under consideration in order to ensure the overall security of the implementation:

- The private key linked to the certificate should be protected against unauthorised access. Thus, regardless of security measures and policies implemented by the Member States, it is highly recommended not to remove the password protection of the private key.

Finally, the latest stable software versions of the components handling the HTTPS communication should always be used. Member States that have performed tests with 3rd party technology releases may publish through PoC their test results and the releases they are considering as stable (or not).

1.12.18 *Summary*

The following table summarises this *risk treatment plan* defined in this document.

The table indicates the suggested priority for implementation for each measure analysed above:

- Measures indicated with HIGH priority are those that need to be implemented by the time ECRIS is ready to be used as a production system, thus by April 2012.
- Measures of MEDIUM priority are those that are proposed to be implemented at a later phase to further increase the degree of security of ECRIS.
- Measures of LOW priority are those that can be omitted without having a significant impact on the degree of security.

In addition to the priorities, the following table gives for each measure a summary of the proposed implementation and references to relevant sections of the analysis given in this document. Finally, the table indicates who is responsible for the definition of detailed specifications of each measure and who is responsible for the implementation of these specifications.

ID	Measure	Priority	Suggested Implementation	Responsibility for Specifications	Responsibility for Implementation
C1	Test of the availability of the Member States' ECRIS sites and applications	HIGH	Decentralised Testing of Availability of Member States' Sites	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C2	Logging of the operations	HIGH	Decentralised Logging of Operations	iLICONN Project team (specifications be provided in "Logging, Monitoring and Statistics Analysis" document)	Member States ECRIS central PoC
C3	Signature of the request	LOW	Not recommended for immediate implementation. *WS-Security* or Custom digital cryptographic signatures could be reasonable choices (see sections 1.12.4 and 1.12.9)	-	-

C4	Sending of an automatic signed acknowledge message	HIGH	Using *SOAP* return code as automatic acknowledge	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C5	Retransmission process	HIGH	To be described in the "Detailed Technical Specifications"	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C6	Use of encryption	HIGH	HTTPS with one-way authentication (HTTPS with mutual authentication to be reconsidered in later versions of ECRIS).	iLICONN Project team ("HTTPS with one-way authentication" specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C7	Procedure for configuration changes (versioning)	HIGH	Versioning principles described in the "Technical Architecture". Change management to be handled by central body.	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents) Member States	Member States ECRIS central PoC

C8	Set-up of an ECRIS central PoC	HIGH	Definition of Central Body	Member States	ECRIS central PoC
C9	Capacity planning	HIGH	Establishing Limits in Message Exchanges	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C9	Capacity planning	MEDIUM	Network Bandwidth Monitoring	Member States sTESTA provider (European Commission)	Member States sTESTA provider (European Commission)
C10	Policy for the use of attachments	HIGH	Establishing Limits in Use of Attachments	iLICONN Project team (specifications provided in the *ECRIS Technical Specifications* documents)	Member States
C11	Memorandum of Understanding (MoU)	MEDIUM	Out of the scope of this project.	Member States ECRIS central PoC	Member States ECRIS central PoC

C12	Routing ACL	HIGH	Out of the scope of this project.	Member States ECRIS central PoC	Member States ECRIS central PoC
C13.a	One-way authentication	HIGH	HTTPS with one-way authentication	iLICONN Project team (specifications to be given in the ECRIS Technical Specifications document)	Member States ECRIS central PoC
C13.b	Mutual authentication	MEDIUM	HTTPS with mutual authentication; to be implemented in later versions of ECRIS	iLICONN Project team (specifications to be given in the ECRIS Technical Specifications document)	Member States ECRIS central PoC
C14	Use of cryptographic techniques to verify the integrity of the received data	HIGH	HTTPS with one-way authentication at first. HTTPS with mutual authentication to be considered in later versions of ECRIS	iLICONN Project team (specifications to be given in the ECRIS Technical Specifications document)	Member States ECRIS central PoC

Table 7 – Summary of the Risk Treatment Plan

2 ANNEX I – THREATS IN EBIOS KNOWLEDGE BASE

The following table lists all threats of the EBIOS Knowledge Base [5] and identifies the threats that are applicable to the ECRIS security analysis. The threats that are applicable to this study are marked in bold.

EBIOS Threat ID	Description	Applicability
Threats on hardware		
M.1.	Misuse of hardware facilities	All hardware-related threats are out of the scope of this security analysis
M.2.	Spying on hardware	
M.3.	Exceeding the operational limits of hardware	
M.4.	Damage of hardware	
M.5.	Changes in hardware	
M.6.	Loss of hardware	
Threats on software		
M.7.	**Misuse of software system**	Although security aspects related to the use of software is not in the scope of this security analysis, ECRIS specifications can partially address this threat as they specify logging of operations, which can be used for accountability purposes.
M.8.	Unauthorised analysis of software system	Out of scope as it is the responsibility of the Member States to provide sufficient controls to secure their assets (including software).
M.9.	**Exceeding the limits of software system**	Although security aspects related to the use of software is not in the scope of this security analysis, ECRIS specifications are related to this threat as they specify part of the input to the software.
M.10.	Partial or complete disruption of software functionality	Out of scope as it is the responsibility of the Member States to provide sufficient controls to secure their assets (including software).
M.11.	**Changes to the software system**	Although security aspects related to the use of software is not in the scope of this security analysis, ECRIS specifications are related to this threat as they specify part of the input to the software.
M.12.	Loss of software system	Out of scope as it is the responsibility of the Member States to provide sufficient controls to secure their assets (including software)
Threats on data channels and telephony		
M.13.	**Man-in-the-middle attack on a data channel or telephone connection**	This threat is in the scope of the security analysis as it applies to the communication network used to exchange data between Member States
M.14.	**Passive listening on a data channel or telephone connection**	This threat is in the scope of the security analysis as it applies to the communication network used to exchange data between Member States

M.15.	**Saturation of a data channel or telephone connection**	This threat is in the scope of the security analysis as it applies to the communication network used to exchange data between Member States
M.16.	Damage on a data channel or telephone connection	Out of the scope since it is the responsibility of the Member States or network providers to protect the communication channels
M.17.	Change to a data channel or telephone connection	Out of the scope since it is the responsibility of the Member States or network providers to protect the communication channels
M.18.	Loss of a data channel or telephone connection	Out of the scope since it is the responsibility of the Member States or network providers to protect the communication channels
Threats on persons		
M.19.	**Inappropriate assignment of activities to a person**	Although security aspects related to the management of personnel are not in the scope of this security study, this threat implies possible unintended action of a user, which could result in misrouting of data
M.20.	Spying on a person from a distance	The security aspects related to persons is not in the scope of this security analysis
M.21.	Exceeding the capacity of a person	The security aspects related to persons is not in the scope of this security analysis
M.22.	Damage to a person	The security aspects related to persons is not in the scope of this security analysis
M.23.	**Influence on a person**	Although security aspects related to the management of personnel are not in the scope of this security study, ECRIS specifications can partially address this threat as they specify logging of operations, which can be used for accountability purposes.
M.24.	Departure of a person	The security aspects related to persons is not in the scope of this security analysis
Threats on paper documents		
M.25.	Misuse of paper documents	All hardware-related threats are out of the scope of this security analysis
M.26.	Spying on paper documents	
M.27.	Damage to paper documents	
M.28.	Loss of paper documents	
Threats on interpersonal channels		
M.29.	Manipulation via an interpersonal channel	All threats to interpersonal communication are out of the scope of this security analysis
M.30.	Spying on an interpersonal channel	
M.31.	Saturation of an interpersonal channel	
M.32.	Damage to an interpersonal channel	
M.33.	Changes in an interpersonal channel	
M.34.	Loss of an interpersonal channel	

Table 8 – EBIOS Threats